ISSUES AND SOLUTIONS: -

1. Windows Email Sign-In Required: -

Soln: - [How to bypass the Microsoft Account requirement during Windows setup - gHacks Tech News](https://www.ghacks.net/2023/01/26/how-to-bypass-the-microsoft-account-requirement-during-windows-setup/)

Used **method 3** to bypass email sign-in

1. Disabling Windows Security Group Policy Permanently: -

Soln: - [How to permanently disable Windows Defender Real Time Protection with GPO? - Super User](https://superuser.com/questions/1757339/how-to-permanently-disable-windows-defender-real-time-protection-with-gpo)

1. No Internet Available in VM: -

Unable to solve. Created a new VM.

1. Didn’t understand what is fakenet: -

Soln: - Bard

FakeNet is a network simulation tool that is used in malware analysis. It allows malware analysts to run malware samples in a safe environment, without the risks of an Internet connection. FakeNet simulates a network of legitimate services, such as HTTP, DNS, and FTP. This allows malware analysts to see how the malware interacts with these services, and to capture network traffic for further analysis.

FakeNet is a valuable tool for malware analysis because it can help analysts to:

* Identify malware's functionality: By observing how the malware interacts with simulated services, analysts can learn about the malware's capabilities.
* Capture network signatures: By capturing network traffic, analysts can identify the malware's C2 servers, command-and-control traffic, and other network indicators.
* Mitigate the risks of malware: By running malware in a safe environment, analysts can mitigate the risks of the malware infecting their systems or networks.

FakeNet is a free and open-source tool that is available for Windows and Linux. It is a powerful tool that can be used to improve the effectiveness of malware analysis.

Here are some of the benefits of using FakeNet in malware analysis:

* It allows malware analysts to run malware samples in a safe environment, without the risks of an Internet connection.
* It can help analysts to identify malware's functionality and capture network signatures.
* It is a free and open-source tool.

Here are some of the limitations of using FakeNet in malware analysis:

* It can only simulate a limited number of network services.
* It may not be able to capture all of the network traffic that is generated by malware.
* It may not be able to detect all of the malware's capabilities.

Overall, FakeNet is a valuable tool for malware analysis. It can help analysts to identify malware's functionality, capture network signatures, and mitigate the risks of malware. However, it is important to be aware of the limitations of the tool.

1. Virtual Machine froze after few minutes of inactivity: -

Enabled 3D acceleration in VM’s settings.

1. Internet in my virtual machine broke after I ran fakenet: -

Fakenet basically reconfigures your dns settings. So, to reset it follow this video: -

https://youtu.be/2K99NpRVQvM